

FRAUD ALERT

**NATIONAL CREDIT UNION ADMINISTRATION
1775 DUKE STREET, ALEXANDRIA, VA 22314**

DATE: October 2010

Fraud ALERT NO.: 10-Fraud-01

TO: Federally-Insured Credit Unions

SUBJ: Phishing Attempt – E-mail Solicitation Using NCUA Address

Dear Board of Directors:

The purpose of this fraud alert is to inform all federally-insured credit unions about a recent phishing attempt to obtain member credit card account numbers, expiration dates and electronic signatures. In cases reported to NCUA, the perpetrator(s) sent fraudulent e-mails, representing to be from the NCUA, to credit union members and the general public. The emails state the NCUA will add \$50.00 to the member's account for taking part in a survey. The link embedded in the message directs members to a counterfeit version of NCUA's website with an illicit survey that solicits credit card account numbers and confidential personal information.

We are highly concerned about the risk of imitating the NCUA website and the use of the NCUA official logo to potentially make the scam appear more authentic to unsuspecting members. NCUA will never ask credit union members or the general public for personal account or personally identifiable information as part of a survey. Any e-mail that alleges to be from NCUA and asks for account information is fraudulent and should be treated as suspicious. We have taken steps to shut this site down, but credit union members should remain alert to possible variations of this fraudulent e-mail.

Credit union management should remain vigilant and instruct employees to monitor and identify any fraudulent activities due to this phishing attempt. Credit union personnel should continue to educate members regarding the signs of any such fraudulent activity. End users who clicked on any of the e-mail links should consult with a computer security or anti-virus specialist to assess the need to re-install a clean image of the computer system. Credit Unions should also encourage members to take the following additional precautions:

- Scan affected computers using updated anti-virus software.
- Enable automatic updates for anti-virus software and computer operating systems.
- Install security patches for common software applications promptly.

- Be aware that phishing e-mails frequently have links to Web pages that host malicious code and software.
- Do not open unsolicited or unexpected e-mail attachments.
- Do not follow Web links in unsolicited e-mails from apparent federal banking agencies, instead, bookmark or type the agency's Web address.
- Call the agency using a known and appropriate telephone number to verify the legitimacy of the message and attached file.

Members affected by this scam, and variants of this scam, should be advised to forward the entire e-mail message to Phishing@ncua.gov. Additionally, formal complaints concerning any suspected fraudulent e-mail can be filed with the Internet Fraud Complaint Center (IFCC) at www.ic3.gov. The IFCC is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center.

NCUA Rules & Regulations Part 748, Appendix B addresses breaches of credit union or credit union service provider's systems which compromise member information. Credit union management must assess the potential for the incident to cause harm or substantial inconvenience to the member. Based on management's risk-based analysis of the incident, the following actions may be necessary:

- Contain and control the incident (monitor, freeze, or close affected accounts while preserving records and other evidence).
- Notify members of the incident as specifically outlined in Part 748 Appendix B.
- File a Suspicious Activity Report in accordance with established regulation.
- Notify the appropriate NCUA Regional Director (or State Supervisory Authority).
- Contact and file a report with local law enforcement authorities.

NCUA will continue to follow this issue and provide you with additional information as warranted. In the meantime, if you have any questions, please contact your District Examiner, Regional Office, or State Supervisory Authority.

Sincerely,

/s/

Melinda A. Love
Director of Examination & Insurance